REMARKS

Claims 1-26 were pending in this case, and were rejected. Claims 1-3, 9, 12, 14-16, 22 and 24 have been amended, and reconsideration of the claims is respectfully requested. Furthermore, new claims 27-30 have been added.

A. *Rejection Under 35 U.S.C. § 103*

Claims 1-26 were rejected under § 103(a) as being unpatentable over U.S. Patent No. 5,819,226 to Gopinathan et al. in view of Schott (dialog file 148, accession No. 07947406). Claim 1 has been amended to recite "comparing the contact event information with fraud information used in known frauds and stored in a database to determine if there is a fraud match between the contact event information and the fraud information". As indicated on page 5 of the application, lines 25-27, the fraud information may include personal information, such as addresses, phone numbers, and social security numbers used in known frauds. Other examples of fraud information are provided on page 5, line 27, through page 6, line 13.

Claim 1 has been further amended to recite "sending a fraud alert to the client if there is a fraud match between the contact event information and the fraud information." Thus, if an element of the contact event information matches an element of the fraud information, a fraud alert is sent to the client.

None of the cited references, either alone or in combination, disclose this combination of steps. By contrast, Gopinathan et al. '226 discloses a system and method that use "a predictive model such as a neural network to evaluate individual customer accounts and identify potentially fraudulent transactions based on learned relationships among known variables." (*See* col. 2, ll. 29 *et seq.*). The system and method of Gopinathan et al. '226 do not involve comparing contact event information with fraud information used in known frauds to determine if there is a fraud match. Nor does Schott cure the deficiencies of Gopinathan et al. '226. Thus, claim 1 and dependent claims 2-13 are believed to be allowable. Claims 2, 3, 9 and 12 have, however, been amended to address informalities.

Claim 14 has been amended to recite that the computer software compares the contact event information with "fraud information used in known frauds and stored in the database to determine if there is a fraud match between the contact event information and the fraud information". Furthermore, claim 14 has been amended to recite that the communication network is "in communication with the database for sending a fraud alert to the client in real time if there is a fraud match between the contact event information and the fraud information." Thus, claim 14 and dependent claims 15-22 and 24 are believed to be allowable for the reasons discussed above with respect to claim 1. Claims 15, 16, 22 and 24 have, however, been amended to address informalities.

B. *New Claims*

New claims 27-30 have been added to recite additional aspects of the invention.

C. *Conclusion*

Applicants have made a genuine effort to respond to the Examiner's objections and rejections in advancing the prosecution of this case. Applicants believe all formal and substantive requirements for patentability have been met and that this case is in condition for allowance, which action is respectfully requested.

A check in the amount of $418 is enclosed to cover the two-month petition for extension of time fee ($400) and the additional claim fee ($18). Please charge any additional fees or credit any overpayments as a result of the filing of this paper to our Deposit Account No. 02-3978 as authorized by the original transmittal letter in this case.

The Examiner is requested to telephone the undersigned to discuss prompt resolution of any remaining issues necessary to place this case in condition for allowance.

Respectfully submitted,

JULIE A. GESCHWENDER ET AL.

By

MARK E. STUENKEL
Reg. No. 44,364
Attorney/Agent for Applicants

Date: *December 3, 2001*

BROOKS & KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075
Phone: 248-358-4400
Fax: 248-358-3351

Attachment

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In The Claims

1. (Amended) A method for detecting purchasing card fraud during all phases of a purchasing card life cycle, the method comprising:

obtaining contact event information from a client during a contact event;

comparing the contact event information with fraud information used in known frauds and stored in a database to determine if there is a fraud match between the contact event information and the fraud information; and

sending a fraud alert to [a] the client [in real time for communicating to the client that] if there is a fraud match [has occurred] between the contact event information and the fraud information.

2. (Amended) [A] The method of claim 1 wherein obtaining contact event information further comprises obtaining a customer's name, [a customer's] social security number, and [customer's] address[, and a customer's fraud history].

3. (Amended) [A] The method of claim 1 [wherein comparing contact event information with a fraud database] further [comprises comparing contact event information with a fraud database having] comprising receiving the fraud information at the database from a plurality of fraud information sources.

9. (Amended) The method of claim 1 wherein sending [an] a fraud alert further comprises sending an account record to an online queue to be monitored by the client.

12. (Amended) The method of claim 11 wherein [the] scoring the fraud match further comprises predicting a likelihood of a fraudulent takeover of a cardholder account.

14. (Amended) A system for detecting purchasing card fraud during all phases of a purchasing card life cycle, the system comprising:

a computer database for receiving contact event information from a client;

computer software in communication with the computer database for comparing the contact event information with fraud information used in known frauds and stored in the database to determine if there is a fraud match between the contact event information and the fraud information; and

a communication network in communication with the database for sending a fraud alert to [a] the client [in real time for informing the client that] if there is a fraud match [has occurred] between the contact event information and the fraud information.

15. (Amended) [A] The system of claim 14 wherein the contact event information [further] comprises a customer's name, [a customer's] social security number, and [customer's] address[, and a customer's fraud history].

16. (Amended) [A] The system of claim 14 wherein the fraud database [has] is adapted to communicate with a plurality of fraud information sources.

22. (Amended) The system of claim 14 wherein the fraud alert [is] includes an account record which is sent to an online queue monitored by [a] the client.

24. (Amended) The system of claim 14 [further comprising scoring] wherein the computer software is operative to score the fraud match to assist in the fraud determination process.